CLAIMS

What is claimed is:

1. A method, comprising:

authenticating, during a pre-boot phase of a client, a boot server on which an operating system (OS) boot image is stored;

downloading an OS boot image from the boot server if it is authenticated; and

loading the OS boot image on the client;

2. The method of claim 1, wherein the boot server is authenticated by comparing a shared secret stored by the client with a corresponding shared secret stored by the boot server.

3. The method of claim 2, further comprising provisioning the shared secret to at least one of the client and the boot server during a one-time provisioning event such that both the client and the boot server have access to the shared secret.

4. The method of claim 3, wherein the shared secret is provisioned using an Extensible Authentication Protocol (EAP message) exchange between an authenticator EAP server and the client.

5. The method of claim 3, wherein the shared secret is provisioned from the client to the server and is formulated via a key that is generated by a trusted platform module stored by the client.

6. The method of claim 3, wherein the shared secret is provisioned using a take ownership protocol under which one of a user or administrator takes ownership of a computer system by providing authentication credentials for that system..

7. The method of claim 6, wherein the take ownership protocol comprises provisioning authentication credentials via one of the following: provisioning authentication credentials on the client via an out-of-band channel, enabling a user to enter authentication credentials via a local console, and imprinting the client with authentication credentials via remote entry of the authentication credentials by a system administrator.

8. The method of claim 1, wherein the boot server is authenticated using an authenticated dynamic host configuration protocol (DHCP) message exchange process.

9. The method of claim 1, further comprising authenticating the client prior to allowing a client to download an OS boot image.

10. The method of claim 9, wherein the client is authenticated using an authenticated dynamic host configuration protocol (DHCP) message exchange process.

11. The method of claim 1, wherein the boot server is authenticated by performing the operations of:

encrypting the shared secret stored at the client;

passing the encrypted shared secret to one of the boot server and an authentication proxy for the boot server;

decrypting the encrypted shared secret at said one of the boot server and the proxy for the boot server; and

comparing a shared secret stored at said one of the boot server and the authentication proxy for the boot server with the encrypted shared secret that is decrypted.

12. The method of claim 1, further comprising:

generating a session key; and

employing the session key for encryption and decryption of data transferred between the boot server and the client.

13. The method of claim 12, further comprising:

updating the session key at some point during download of the OS boot image; and

employing the updated session key for encryption and decryption of data transferred between the boot server and the client while downloading a subsequent portion of the OS boot image.

14. The method of claim 1, wherein the shared secret is derived from the combination of a user login and a password corresponding to the user login.

15. A computer system, comprising:

a processor;

memory, coupled to the processor;

a network interface, coupled to the processor;

a firmware storage device, coupled to the processor; having firmware instructions stored therein that when executed on the processor cause operations to be performed, including:

interacting with a boot server via messages sent to and received from the boot server through the network interface during a pre-boot initialization phase of the computer system to authenticate the boot server;

downloading an OS boot image from the boot server if it is authenticated; and

loading the OS boot image into the memory.

16. The system of claim 15, wherein the boot server is authenticated by comparing a shared secret stored by the computer system with a corresponding shared secret stored by the boot server.

17. The system of claim 15, wherein the boot server is authenticated using an authenticated dynamic host configuration protocol (DHCP) message exchange process.

18. The system of claim 17, wherein execution of the firmware instructions further performs authentication of the computer system via the authenticated DHCP message exchange process.

19. The system of claim 15, wherein the OS boot image is served from the boot server in an encrypted form, and execution of the firmware instructions further performs the operation of decrypting the OS boot image.

20. The system of claim 19, wherein execution of the firmware instructions further performs the operation of interacting, via a message exchange, with the boot server to agree on a session key that is used to encrypt and decrypt the OS boot image.

21. The system of claim 15, further comprising a trusted platform module, operatively coupled to the processor and storing an ownership token that is used to formulate the shared secret.

22. The system of claim 21, wherein the ownership token comprises a key that is instantiated via the trusted platform module.

23. A machine-readable media providing instructions to perform operations on a computer system, including:

interacting with one of a boot server or authentication server via messages generated by the computer system and sent to the boot server or authentication server and messages received from the boot server or authentication server and processed by the computer system during a pre-boot initialization phase of the computer system to authenticate the boot server;

sending a request to the boot server to download an OS boot image from the boot server if it is authenticated;

downloading the OS boot image from the boot server; and

loading the OS boot image into memory of the computer system.

24. The machine-readable media of claim 23, wherein the media comprises a firmware storage device and the instructions comprise firmware instructions.

25. The machine-readable media of claim 23, wherein execution of the instructions performs the further operation of broadcasting a boot server discovery message to locate the boot server.

26. The machine-readable media of claim 23, wherein the boot server is authenticated by comparing a shared secret stored by the computer system with a corresponding shared secret stored by the boot server.

27. The machine-readable media of claim 26, wherein execution of the instructions performs the further operations of:

encrypting the shared secret stored at the computer system; and

sending the shared secret in encrypted form to one of the boot server or an authentication proxy for the boot server.

28. The machine-readable media of claim 23, wherein the boot server is authenticated using an authenticated dynamic host configuration protocol (DHCP) message exchange process.

29. The machine-readable media of claim 28, wherein execution of the instructions further performs authentication of the computer system via the authenticated DHCP message exchange process.

30. The machine-readable media of claim 23, wherein execution of the instructions further performs the operations of:

generating a user interface on the computer system via which a user can enter authentication credentials;

generating a shared secret based on the authentication credentials; and

sending the shared secret to the boot server or authentication server.